REMARKS

Claims 1-24 are pending in the application. Claims 1-24 have been rejected.

Claim Rejections under 35 U.S.C. § 102(e)

Claims 1-5, 10, 11, 13-16 and 18-24 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent 6,690,795 to Richards (hereinafter "Richards"). Applicants respectfully disagree for the reasons and explanations set forth below.

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." M.P.E.P. § 2131 (Aug. 2001) (*quoting Verdegaal Bros. v. Union Oil Co. of California,* 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)). "The identical invention must be shown in as complete detail as is contained in the . . . claim." *Id.* (*quoting Richardson v. Suzuki Motor Co.,* 868 F.2d 1226, 1236, 9 USPQ2d 1051, 1053 (Fed. Cir. 1987)). In addition, "the reference must be enabling and describe the applicant's invention sufficiently to have placed it in possession of a person of ordinary skill in the field of the invention." *In re Paulsen,* 30 F.3d 1475, 1479, 31 USPQ2d 1671, 1673 (Fed. Cir. 1994).

Applicants respectfully submit that claims 1-5, 10, 11, 13-16 and 18-24 are not anticipated by Richards for the reasons and explanations set forth below.

With respect to amended claim 1 Applicants respectfully submit that Richards does not disclose all the limitations of claim 1. In particular, Richards does not disclose "sending the first key on a broadcast channel".

Richards discloses an encryption system for restricted-access television systems. A television program is delivered to a customer in the form of a stream of digital data, along a data link, such as a coaxial cable. (Col. 2, lines 41-43). The channels typically have sufficient bandwidth to carry multiple television programs. (Col. 2, liens 45-47). Time multiplexing is used to transmit the channel in the form of digital data packets. (Col. 2, lines 52-56). Each customer has a set top box which includes a decoder to decode and process the packets. (Col. 2, lines 63-65). The data packets are distributed in parallel to all customers. All customers receive all the packets for all programs broadcast. However, customers are only granted access to the specific

programs provided in their subscriptions. (Col. 3, lines 5-11). The Access Control system distributes decryption keys to customers. The distribution is typically accomplished by sending each customer the decryption keys in encrypted form. (Col. 4, lines 55-59). Each customer's set top box is assigned a unique key. The decryption keys are encrypted using the customer's set top box key. This results in each customer obtaining only the decryption keys for the programs intended for that customer. (Col. 4, lines 59-62). The key, SK, is itself encrypted using another key, PK. Each customer receives two data words. The key SK is encrypted using PK, a program key. PK is encrypted using the unique key of the customer's set top box. (Col. 9, lines 12-18). Both keys, SK and PK are delivered by an out of band channel. (Col. 9, lines 21-22). Key SK is encrypted using PK as a key and is decrypted at the customer using actual PK to produce actual SK and thus produces the content. (Col. 9, lines 25-31). Therefore, Richards does not disclose "sending the first key on a broadcast channel". Applicants respectfully submit that amended claim 1 is not anticipated by Richards.

Claims 11 and 22-24 are allowable for the same reasons given above for claim 1.

Claim 13 is allowable as depending directly from allowable claim 11 and also contains additional limitations.

Claims 2, 3 and 14 are allowable as depending directly or indirectly from allowable claim 1 or claim 11.

Claim 4 depends indirectly from allowable claim 1 and contains additional limitations. Applicants submit that claim 4 is allowable as depending from allowable claims 1 and 2.

Claim 5 depends indirectly from allowable claim 1 and contains additional limitations. Applicants submit that claim 5 is allowable as depending from allowable claims 4, 2, and 1.

Claim 10 depends directly from allowable claim 1 and contains additional limitations. Applicants submit that claim 10 is allowable as depending from allowable claim 1.

Claim 15 is allowable for the same reasons given above for claim 1.

Claims 16, 18, 19, 20, and 21 are allowable as depending directly or indirectly from allowable claim 15.

Claim Rejections under 35 U.S.C. § 103

Claims 6-9, 12, and 17 were rejected as being unpatentable over U.S. Patent 6,690,795 to Richards (hereinafter "Richards"). This rejection is respectfully traversed.

To establish a prima facie case of obviousness, the prior art reference (or references when combined) must teach or suggest all the claim limitations. "The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art, not in Applicants' disclosure." In re Vaeck, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Applicants respectfully submit that a prima facie case of obviousness has not been established regarding claims 6-9, 12, and 17 because the prior art cited does not teach or suggest all the claim limitations.

Claim 6 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Richards, as applied to claim 4 above, and in further view of "FOLDOC, Free On-Line Dictionary of Computing" by LinuxGuruz.

Claim 4 depends directly from claim 1 and includes additional limitations. As discussed above, Richards does not disclose or suggest the limitation "sending the first key on a broadcast channel". In Richards both keys are sent using out-of-band signaling directly to each subscriber's set top box. Furthermore, Richards is directed to cable television systems which transmit all programs to users and rely on specific decryption keys to decode only the content permitted by the user's subscription package. It would not be obvious to combine a method for transmitting keys for cable television programs with an internet transport medium, such as Internet Protocol packets. Additionally, claim 6 is allowable as depending from allowable claim 4.

Claims 7-9 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Richards, as applied to claim 3, above, in further view of Applied Cryptography, Second Edition, by Schneier. Because neither Richards nor Schneier teaches or suggests the limitation "sending or receiving a first key on a broadcast channel" claim 3 is not anticipated by the combination. Furthermore, the combination of Richards and Schneier teaches away from Applicants' invention. Schenier teaches that no key should be used for an indefinite period and also teaches that keys should be kept secure. (p. 182, § 8,9) it would not be obvious to send a key, even an

encrypted key on a broadcast channel. Therefore, claim 7 is allowable, both for the reasons given above for claims 1 and 3, and independently.

Claims 8 and 9 are allowable as depending directly or indirectly from allowable amended claim 7.

Claims 12 and 17 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Richards, as applied to claims 11 and 15 above, in further view of U.S. Patent 6,073,122 to Wool (hereinafter "Wool"). Applicants respectfully submit that claims 12 and 17 are allowable for the reasons given above for claims 11 and 15, and as depending from allowable amended claims.

REQUEST FOR ALLOWANCE

In view of the foregoing, Applicant submits that all pending claims in the application are patentable. Accordingly, reconsideration and allowance of this application are earnestly solicited. Should any issues remain unresolved, the Examiner is encouraged to telephone the undersigned at the number provided below.

Respectfully submitted,

Dated: March 21, 2005

By: *Roberta A. Young*
Roberta A. Young, Reg. No. 53,813
(858) 658-5803

QUALCOMM Incorporated
5775 Morehouse Drive
San Diego, California 92121
Telephone: (858) 658-5787
Facsimile: (858) 658-2502